IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF

(a) THE PERSON OF SHAWN ADAMS, ANY VEHICLES IN HIS CUSTODY AND CONTROL, AND ELECTRONIC DEVICES AND MEDIA, AS DESCRIBED IN ATTACHMENT A-1; AND

(b) 203 FOREST COVE AYLETT, VIRGINIA 23009, AS DESCRIBED IN ATTACHMENT A-2

Case No. 3:23SW138
3:23SW139
FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Kenneth H. Jordan III, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of the person of SHAWN TRAVIS ADAMS (hereinafter referred to as "ADAMS"), including the passenger compartment and trunk of any vehicle in ADAMS's possession or control, for any electronic devices found on ADAMS's person and/or in ADAMS's possession, as further described in Attachment A-1; and the premises located at 203 FOREST COVE AYLETT, VIRGINIA 23009 (hereinafter referred to as "PREMISES") as further described in Attachment A-2. In particular, this affidavit is made in support of an application for a warrant to search for and seize evidence, instrumentalities, and fruits of violations of 18 U.S.C. § 2252A (Transportation, Distribution, Receipt, and Possession of Child Pornography), as further described in Attachment B.

2. I am a Special Deputy United States Marshal assigned to the Federal Bureau of Investigation (FBI), as a Task Force Officer and have been since 2018. I am assigned to the Richmond Field Office of the FBI in Richmond, Virginia, and am responsible for conducting investigations pertaining to child exploitation. As part of my duties, I have received training regarding the investigation of federal crimes including crimes against children and human trafficking. By virtue of my assignment to the FBI and my employment with the Middlesex County Sheriff's Office I have performed a variety of investigative tasks including, but not limited to, conducting arrests and executing federal search warrants. As a Special Deputy United States Marshal, I am an investigative or law enforcement officer within the meaning of 18 U.S.C. § 2510(7).

3. The facts in this affidavit come from my personal observations and review of records, my training and experience. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

RELEVANT STATUTORY PROVISIONS

4. **Transportation of Child Pornography:** 18 U.S.C. § 2252A(a)(1) provides that it is a crime for any person to knowingly mail, transport or ship any child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer.

5. **Distribution or Receipt of Child Pornography:** 18 U.S.C. § 2252A(a)(2) provides that it is a crime to knowingly receive or distribute any child pornography that has been mailed or using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

6. **Possession of Child Pornography**: 18 U.S.C. § 2252A(a)(5) provides that it is a crime to knowingly possess, or knowingly access with intent to view, any child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

7. **Child pornography or Child abusive material** means any visual depiction, in any format, of sexually explicit conduct where: (A) the production involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital or computer-generated image that is substantially indistinguishable from that of a minor engaged in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

8. **Visual depictions** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which are capable of conversion into a visual image, and data which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

9. **Minor** means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

10. **Sexually explicit conduct** means actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

TECHNICAL TERMS

11. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. **Computer**, as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

b. **Storage Medium**: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

c. **Wireless Telephone**: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

d. **Smartphone**: A portable personal computer with a mobile operating system having features useful for mobile or handheld use. Smartphones, which are

typically pocket-sized (as opposed to tablets, which are larger in measurement), have become commonplace in modern society in developed nations. While the functionality of smartphones may vary somewhat from model to model, they typically possess most if not all of the following features and capabilities: 1) place and receive voice and video calls; 2) create, send and receive text messages; 3) voice-activated digital assistants (such as Siri, Google Assistant, Alexa, Cortana, or Bixby) designed to enhance the user experience; 4) event calendars; 5) contact lists; 6) media players; 7) video games; 8) GPS navigation; 9) digital camera and digital video camera; and 10) third-part software components commonly referred to as "apps." Smartphones can access the Internet through cellular as well as Wi-Fi ("wireless fidelity") networks. They typically have a color display with a graphical user interface that covers most of the front surface of the phone and which usually functions as a touchscreen and sometimes additionally as a touch-enabled keyboard.

e. **SIM Card**: Stands for a "subscriber identity module" or "subscriber identification module," which is the name for an integrated circuit used in mobile phones that is designed to securely store the phone's international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contact information on many SIM cards.

f. **Log Files**: Records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

g. **Internet**: A global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. **Internet Protocol Address (IP address)**: A unique number used by a computer to access the Internet. Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static–that is, long-term–IP addresses, while other computers have dynamic that is, frequently changed–IP addresses. Internet providers use either IP version 4 or more recently IP version 6. IPv4 is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Given the rapid growth of the volume of internet-enabled devices over the past two decades, in early 2011, the Internet Assigned Numbers Authority exhausted the global IPv4 free pool. As such, many providers switched to IPv6, which is a series of eight hexadecimal digits, each separated by colons (e.g., 2001:0db8:0000:0000:0000:ff00:0042:8329).

i. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage devices).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

12. As described above and in Attachment B, this application seeks permission to search for records that might be found on ADAMS's person and on the PREMISES, in whatever form they are found. The warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

13. **Probable Cause:** I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space–that is, in space on the storage medium that is not currently being used by an active file–for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Apart from user-generated files, computer storage media–in particular, computers' internal hard drives–contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file

system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

14. **Forensic Evidence:** As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when,

where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under

investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

15. **Necessity of Seizing or Copying Entire Computers or Storage Media:** In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete

electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements*. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

16. **Nature of Examination**: Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of electronic devices,

including cellular telephones, consistent with the warrant. The examination may require techniques, including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection to determine whether it is evidence described by the warrant.

PROBABLE CAUSE

17. In October 2022 I was assigned to investigate 108 CyberTips[1] that were reported to the National Center for Missing and Exploited Children ("NCMEC") by Synchronoss Technologies Inc. (hereafter "Synchronoss"). Synchronoss provides cloud storage services for Verizon Wireless. These CyberTips indicated that an employee of Synchronoss had reviewed these images and flagged them as material depicting the sexual exploitation of minors. I personally reviewed all images in these 108 CyberTips. Based on my training and experience I determined that 1304 of the images constituted child pornography as that term is defined in 18 U.S.C. § 2256(8). Three examples of the images I reviewed are described below:

a. **File name: 1f0be326098545e29a1f9f129418fb3b_f578802eee154bcbaa0036a6f0dbdcf12f101ad4c4d38f09080598fbc09db015**: This image file, which is associated with CyberTip **No. 128717754** and was uploaded on July 11, 2022, depicts a male of the approximate age of 12 years old. He is on a bed laying back on some pillows,

[1] Internet service providers frequently provide reports regarding child abuse and child exploitation on their platforms to the National Center for Missing and Exploited Children ("NCMEC") or its international partner, the International Center for Missing and Exploited Children. *See* 18 U.S.C. § 2258A. These reports, called CyberTips, provide useful information about when and how these providers become aware of violations of their terms of service and may provide information about other accounts associated with a subject's account. For CyberTips relating to the distribution, receipt or possession of child pornography, providers typically include copies of the offending images in their report submissions to NCMEC.

has his hands behind his knees and is pulling them back and apart, exposing his anus and erect penis.

b. **File name: 1f0be326098545e29a1f9f129418fb3b_5717ded91dcb33cca3a2114cf2c532d4b40796905b2c16ead48700df85f0aaf9**: This image file, which is associated with CyberTip **No. 119953105** and was uploaded on March 15, 2022, depicts a female toddler of approximately one to two years of age lying with her legs outstretched and sucking on a pacifier while being penetrated vaginally by an inanimate object.

c. **File name: 1f0be326098545e29a1f9f129418fb3b_cec7f6a10b001f2900227988f337695ccb3983e765d1da8abd1553000df0e8c4.zip:** This image file, which is associated with CyberTip **No. 116588788** and was uploaded on January 12, 2022, depicts a female of the approximate age of six months old and lying on her back. An unidentified individual uses their index and middle fingers to spread the lips of the vagina wide apart exposing deep into the baby's vagina.

18. Based on the information contained in these tips, a subpoena was issued to Verizon for records for phone number **804-767-0266.** My review of records obtained pursuant to subpoenas issued to Verizon Wireless determined that the phone number used to upload the child pornography images in all 108 CyberTip's was **804-767-0266.** Verizon provided information for telephone number **804-767-0266** indicating that the account subscriber is SHAWN ADAMS, having the address of 203 Forest Cove, Aylett, Virginia, email account of superman4life1982@gmail.com, and last four digits of his Social Security number of 5262.

19. Additionally, Verizon provided information that the device associated to the above telephone number was a Note 20 Ultra 5G Black 128GB, which is a Samsung Galaxy mobile device employing the Android operating system. Identification numbers for that device

included an IMEI of 356556776814940 and IMSI of 311480657747842[2]. The account was opened on October 6, 2021.

20. On February 2, 2023, this Court issued a search warrant, Case No. 3:23-sw-16, for ADAMS's Synchronoss account, which I promptly served on Synchronoss. On February 3, 2023, I received an email from a Synchronoss employee informing me that ADAMS account had been deactivated on July 12, 2022 (which is the day after the most recent CyberTip). Even though the account had been deactivated, Synchronoss still possessed contents of the account because it had received a preservation request before the account had been closed. The Synchronoss employee also stated that Synchronoss's collection process is automated and cannot target specific dates. Because Synchronoss cannot filter searches by date they requested an amended warrant without a date range so that they could properly comply with the warrant.

21. On February 9, 2023, another search warrant was obtained, Case No. 3:23-sw-29, to address the request of Synchronoss to omit specific target dates. This warrant was executed on February 10, 2023, and the digital records were returned to me by email. I examined the return and found it to contain 2,483 image files, including videos, pictures and PDF's. I have reviewed the files and have found thus far that over 1,300 are images of child pornography as that term is defined in 18 U.S.C. § 2256(8). I still have approximately 2,000 images/videos to review.

---

[2] **IMEI** stands for International Mobile Equipment Identity, which is a numeric identifier, usually unique, for many mobile phone devices. The IMEI is encoded into the device by the manufacturer. The IMEI only identifies the mobile device itself, not a particular subscriber, and cannot be transferred to another device. **IMSI** stands for International Mobile Subscriber Identity, which is a number that uniquely identifies every user of a cellular network. An IMSI is stored on a device's SIM card and can be transferred to another device that has a SIM card slot.

Identification of ADAMS and Further Investigation

22. Through queries of law enforcement databases, TLOxp[3], the Virginia Employment Commission, and the Virginia Department of Motor Vehicles, I identified the occupant of the PREMISES as SHAWN TRAVIS ADAMS ("ADAMS"), date of birth December 28, 1982, SSN XXX-XX-5262, with a listed address of the PREMISES.

23. Between March 16 and March 27, 2023, investigators conducted surveillance at the PREMISES on several separate occasions. During the surveillance, investigators observed a male individual fitting ADAMS description entering and exiting the PREMISES. Investigators were also able to observe the vehicle registered to SHAWN ADAMS, a black, four-door 2020 Ford Escape, being operated and parked in the driveway at the PREMISES. Additionally, investigators determined that ADAMS works at Atlantic Vision Partners, located at 2010 S. Crestwood Ave., Suite 128, Richmond, Virginia, 23226.

24. During a three-week period from July 17, 2023, to August 11, 2023, ADAMS did not follow his previously established daily routine and his whereabouts were unknown to law enforcement. On August 11, 2023, an FBI surveillance team observed ADAMS leaving his place of employment and getting into an Uber. The team followed him to 12426 Hogans Pl. Chester Virginia, 23836. While there ADAMS met an individual who handed him keys to a maroon Honda Accord displaying VA registration, UHR-7682. Investigators observed ADAMS drive the Honda Accord back to his place of employment. I determined through additional investigation that on July 16, 2023, ADAMS was involved in a single-vehicle crash on route 360 in King

---

[3] TLOxp is a subscription-based service offered by TransUnion that enables users to conduct advanced searches across multiple public and proprietary databases.

William County and his car had to be towed from the scene due to the damage. On August 14, 2023, investigators observed ADAMS departing the area of his residence in the same Honda Accord described above and driving to his place of employment. Investigators later observed ADAMS leave his workplace at around 4:00 p.m. on August 14 and return home to the PREMISES in the Honda Accord.

25. On March 5, 2023, I sent a subpoena to Verizon Wireless to ascertain the status of the device listed in paragraph 19 above. On March 12, 2023, I received a return from Verizon Wireless that indicated that ADAMS had disconnected service with Verizon on this device on July 12, 2022

26. Utilizing TLOxp, I found another cell phone number associated with ADAMS, specifically, **804-696-1715**. This was determined to be a number assigned by T-Mobile. On March 12, 2023, a subpoena was sent to T-Mobile for subscriber, device, and account information. On March 16, 2023, I received a return from T-Mobile and found the account belonged to ADAMS, with an address of 203 Forest Cove, Aylett, Virginia, 23009, which is the PREMISES. The activation date of the account was December 15, 2022. I reviewed the call detail records provided and found that the same IMEI associated with the device listed in paragraph 19 above, was captured 13 times as making an outgoing call with cell number **804-696-1715**. The first was recorded on the date the account was opened, December 15, 2022. The most recent was on April 15, 2023. This indicates that the same device handset assigned number **804-767-0266** that was used to upload and store the child pornography images on the Verizon network as described above is now being used to place calls on the T-Mobile network with an assigned number of **804-696-1715.**

27. On August 14, 2023, I conducted a query of the same IMEI number listed in paragraph 19 using the SEARCH.org investigative toolbar. SEARCH is an open-source investigative tool that combines a wide variety of data sets into one tool for enhanced searches of open-source information. Subscriber information is not available through SEARCH; however, my query did show that the pertinent IMEI number is still in active use on the T-Mobile network.

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

28. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereinafter referred to as "collectors").

29. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

30. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, drawings, and/or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature, and sexual aids.

31. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

32. Collectors almost always possess and maintain their "hard copies" of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, many collections are maintained in digital format. Typically, these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and the legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

33. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

34. Collectors prefer not to be without their child pornography for any prolonged periods of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

35. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during nationwide law enforcement initiatives.

36. In sum, collectors of child pornography frequently maintain their collections in a private and secure location such as their residence, often in digital format, for long periods of time. They also maintain information related to their receipt or distribution of such media in that

location, including correspondence with and contact information for other individuals distributing or sharing child pornography.

EVIDENCE INDICATING THAT SHAWN ADAMS IS A COLLECTOR

37. Evidence obtained during this investigation indicates that ADAMS is a likely collector of child pornography. The first indicator is the sheer volume of images. The 108 CyberTips comprised over 1,300 images of child pornography that had been uploaded to ADAMS's Synchronoss cloud account. My initial look at the returns from the follow-on search warrant on ADAMS's Synchronoss account suggests that there are 100's more child pornography images, but as indicated above I have not completed the formal review and categorization of an additional 2,000 images.

38. A second factor reflective of collector behavior was the date range for these image uploads. The 108 CyberTips reflect the fact that on 108 separate days, over the course of approximately seven months, child pornography images were uploaded to the account, beginning December 17, 2021, and ending July 11, 2022. The number of files attached with each upload varied from as few as one file on several days to as many as 260 files on one date in particular. These numbers negate the argument some defendants attempt to assert that a large number of images found on their computer was the result of some automated process that collected a volume of images all at once without a person's input or awareness.

39. A third factor consistent with collector behavior was the relatively uniform nature of the child pornography files. While there were a few image files depicting female minors, the overwhelming majority depicted young boys who were either prepubescent or barely pubescent.

40. A fourth factor suggestive of collector behavior was the presence of numerous mobile phone screen capture images stored in ADAMS's Synchronoss account. Multiple screenshots showed the phone user (presumably ADAMS) engaged in group chats on several

platforms, including ICQ and Facebook. One Facebook group name in particular, which was partially truncated by the screenshot, was "Only Children from Para." Other information on the screenshot, including Spanish language writing, implies that "Paraguay" was the complete word. There were screenshots indicating use of Mega.io, which is a cloud storage service headquartered in New Zealand and known by law enforcement to be used for the storage of child pornography images. There were also screenshots showing the mobile device using the TOR browser[4] to access various images and groups.

41. A final factor indirectly suggesting collector behavior is the set of circumstances associated with the closure of ADAMS's Synchronoss account and the termination of service with Verizon. The last upload of child pornography images to ADAMS's Synchronoss account was July 11, 2022. The next day, July 12, 2022, ADAMS's Synchronoss account was deactivated. Based on my conversation with a Synchronoss employee, once child pornography images are identified their system moves those images into quarantine. Thereafter those images would be unavailable to the account holder. During a related conversation with a Verizon

---

[4] **Tor** is free software for enabling anonymous communications. The name Tor is an acronym for the original software project named "The Onion Router." Tor directs internet traffic through a free, worldwide, overlay network consisting of thousands of relays called "nodes." This network conceals a user's location, identity and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace internet activity back to the actual user: this includes visits to Web sites, online posts, instant messages, and other communication forms. The Tor network can also provide anonymity to websites and other servers. Servers configured to receive inbound connections only through Tor are called **hidden services**. Rather than revealing a server's true IP address (and thus its network location), a hidden service is accessed through something called an onion address, usually via the **Tor Browser**. Tor hidden services are widely used for criminal activity, including the sale and distribution of contraband such as child pornography and illicit drugs.

employee, I learned that Verizon would not have closed ADAMS's account for violation of its terms of service, i.e., the storage of child pornography, without a court order. No such order was issued in this case. It appears, then, that on July 11, 2022, shortly after he made his final upload ADAMS discovered that the previously uploaded child pornography images had been removed from his account. Presumably upon seeing this ADAMS immediately cancelled his Verizon service and later opened an account with T-Mobile.

BIOMETRIC ACCESS TO DEVICES

42. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, iris scans, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. Other device manufacturers such as

Samsung, which makes mobile devices with the Android operating system, have similar fingerprint sensors going by different names.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. Increasingly mobile device manufacturers incorporate this feature into their products. As two examples, Apple's system is called "Face ID" and Samsung's is called "Face recognition." During the facial recognition set-up process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if

such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices may not be able to be unlocked using Touch ID or FaceID when either (1) a certain amount of time has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint or face scan for a certain amount of time and the passcode or password has not been recently entered. Biometric features from other brands carry similar restrictions. The amount of time before the device will require a passcode differs among various mobile phone brands and can even vary between different models and operating systems within the same brand. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

43. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement

personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

CONCLUSION

44. I know from my training and experience, including my own personal experience, that sometimes people will leave their electronic devices, including cell phones, inside their cars when they get out of the vehicle for whatever reason. This happens both intentionally and unintentionally. In my professional experience, I have participated in multiple search warrants during which electronic devices and media containing child pornography have been recovered from the subjects' vehicles. For this reason, it is appropriate to search any vehicle in the custody or control of ADAMS for the evidence described in this affidavit and Attachment B.

45. Based on the forgoing, I submit there is probable cause to believe that any electronic devices found on ADAMS's person and/or in ADAMS's possession, including inside any vehicle in his custody or control, as further described in Attachment A-1; and the PREMISES, as further described in Attachment A-2, contain evidence and instrumentalities of violations of 18 U.S.C. § 2252A (a)(1),(a)(2) and (a)(5) (Transportation, Distribution, Receipt, and Possession of Child Pornography), as further described in Attachment B.

46. Specifically, the evidence suggesting that ADAMS is a collector of child pornography points to a likelihood that evidence of such images will be stored on his cell device and/or electronic media. Additionally, beyond whatever child pornography images that could be recovered from ADAMS's phones and computer(s), there is an equally strong likelihood that

such devices will contain evidence revealing the identity and use of other cloud-based storage accounts containing child pornography images.

Respectfully submitted,

Kenneth H. Jordan III
TFO/Special Deputy U.S Marshal
FBI Richmond Field Office

Sworn and attested to me in my presence:

/s/
Summer L. Speight
United States Magistrate Judge

Date: August 16, 2023
Richmond, Virginia

ATTACHMENT A-1
Property to Be Searched

The person to be searched is SHAWN ADAMS, a male born on December 28, 1982, with brown hair and approximately 5'7", including all personal items and containers, including electronic devices, in his physical possession, on his person, or in areas within his immediate control, including the passenger compartment and trunk of any vehicle in ADAMS's possession or control at the time of the execution of the search warrant.

ATTACHMENT A-2

Property to Be Searched

The property to be searched is **203 Forest Cove Aylett, Virginia 23009**, hereafter referred to as the "PREMISES." The PREMISES is a single-story, single-family home situated at the end of a short driveway. The structure has a light-colored exterior, and multiple entrances/exits. This warrant applies to the main residential structure and the surrounding curtilage, including vehicles. An aerial view and two street-level photographs of the PREMISES are provided below.

ATTACHMENT B

Particular Things to be Seized

1. All records relating to violations of 18 U.S.C. § 2252A (Distribution, Receipt, and Possession of Child Pornography), including:

a. Any and all visual depictions of minors.

b. Any and all address books, names and lists of names and addresses of minors.

c. Any and all records reflecting physical contacts, whether real or imagined, with minors; and

d. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

2. Any computer, electronic device, or storage media, which includes any laptop, desktop, smartphone, cellular device such as a tablet and iPad, and digital camera, all of which are hereafter referred to as a "COMPUTER," that was used as a means to commit the violations described above.

3. For COMPUTER whose seizure is otherwise authorized by this warrant:

a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondences.

b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

c. Evidence of the lack of such malicious software.

d. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence.

e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER.

f. Evidence of the times the COMPUTER was used.

g. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER.

h. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER.

i. Records of or information about Internet Protocol addresses used by the COMPUTER.

j. Records of, or information about, the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

k. Contextual information necessary to understand the evidence described in this attachment.

During the execution of the search of ADAMS person and the PREMISES, as further described in Attachments A-1 and A-2, law enforcement personnel are also specifically authorized to obtain from ADAMS the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person's physical

biometric characteristics will unlock the device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

a. any of the device(s) found at the PREMISES or on ADAMS person,

b. where the device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant Attachments A-1 and A-2,

for the purpose of attempting to unlock the device(s)'s security features in order to search the contents as authorized by this warrant.

While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person for the password to any device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

This warrant authorizes a review of electronically stored information, communications, other records, and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized materials that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no previous or future involvement in the investigation of this matter. The Filter Team will review all seized communications and segregate potentially protected materials, i.e., communications to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team decides that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team.

Your affiant requests the search warrant for the aforementioned items to include the opening and searching of any locked safes, boxes, and compartments.